PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-038029

(43)Date of publication of application : 07.02.1992

(51)Int.Cl. H04L 9/06
G06F 15/00
G09C 1/00
H04L 9/14

(21)Application number : 02-144305

(22)Date of filing : 04.06.1990

(71)Applicant : HITACHI LTD

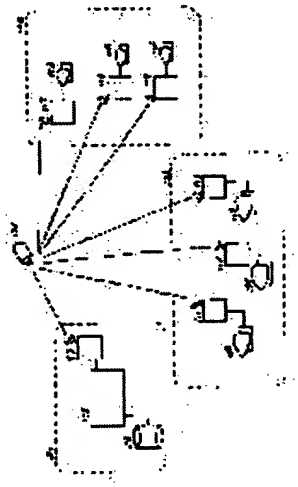
(72)Inventor : FUKUZAWA YASUKO
TAKARAGI KAZUO
NAKAMURA TSUTOMU

(54) INFORMATION SERVICE SYSTEM

(57)Abstract:

PURPOSE: To make a common key generating time of the system almost independent of the increase in number of participants of the system by dividing a receiver terminal equipment into plural groups and devising the system so that only ID information by a group participant for generating a group common key is required in order that each receiver acquires a secret key.

CONSTITUTION: This system consists of plural groups 103,104 each comprising plural reception stations and an information service station 101. The information service station 101 generates a secret key for service information cryptography and uses the secret key to cipher the service information, and generates a common key of each group corresponding to a distribution destination information string comprising each subscriber identifier of each group, uses the common key to cipher the secret key and sends the service information and the secret key to be ciphered respectively by means of multiple address communication. Each reception station receives the information from the information service station 101 and generates a common key of each group from the distribution destination information string for each group and uses the common key to decode a ciphered secret key. When the subscriber identifier is not included in the distribution destination information string of the group, the generation of the common key of the group is inhibited.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平4−38029

⑤1Int.Cl.⁵	識別記号	庁内整理番号	④3公開　平成4年(1992)2月7日
H 04 L 9/06			
G 06 F 15/00	330	7218−5L	
G 09 C 1/00		7922−5L	
H 04 L 9/14			
		7117−5K　H 04 L 9/02　Z	

審査請求　未請求　請求項の数 7　(全11頁)

⑤4発明の名称　情報サービスシステム

⑳特　願　平2−144305
㉒出　願　平2(1990)6月4日

⑦2発明者　福澤　寧子　神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
⑦2発明者　宝木　和夫　神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
⑦2発明者　中村　勤　神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
⑦1出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地
⑦4代理人　弁理士　小川　勝男　外1名

明　細　書

1．発明の名称

情報サービスシステム

2．特許請求の範囲

1．複数の受信局を1つのグループとする複数のグループと、上記複数のグループの複数の受信局に情報を提供する情報サービス局とからなる情報サービスシステムにおいて、

情報サービス局は、情報サービスシステムの加入者の各加入者識別子から構成された配付先情報列を記憶する手段と、サービス情報暗号用の秘密鍵を生成し、上記秘密鍵を用いて、上記サービス情報を暗号化し、上記各グループの配付先情報列に対応した各グループの共通鍵を生成し、各グループの共通鍵を用いて、上記秘密鍵を暗号化し、暗号化されたサービス情報と、暗号化された秘密鍵を同報通信により送出するための手段を有し、

上記各受信局は、情報サービスシステムにおいて各受信局が属する各グループの加入者の各加入者識別子から構成された配付先情報列を記憶する手段と、情報サービス局からの情報を受信するための受信部と、各グループ毎の前記配付先情報列から、各グループの共通鍵を生成する共通鍵生成部と、上記共通鍵を用いて、上記暗号化秘密鍵を復号するための復号部と、各グループの各加入者識別子を記憶するための記憶手段とを備え、

該加入者識別子が該グループの上記配付先情報列に含まれていないときに、上記該グループの共通鍵を生成することを禁止することを特徴とする情報サービスシステム。

2．請求項第1項記載の情報サービスシステムにおいて、

上記各受信局は、情報サービスシステムの、各受信局が属する各グループの識別子と、各受信局が属する各グループの加入者の各加入者識別子から構成された配付先情報列を記憶していることを特徴とする情報サービスシステム。

3．前記受信局側共通鍵生成部、および前記記憶

手段は、前記受信局に着脱可能な回路装置により構成されることを特徴とする請求項第1項，第2項記載の情報サービスシステム。

4．複数の受信局を1つのグループとする複数のグループと、上記複数のグループの複数の受信局に情報を提供する情報サービス局とからなる情報サービスシステムにおいて、

上記情報サービス局は、情報サービスシステムにおける全加入者の識別子を所定の順序で配列した全加入者の識別子情報列を記憶する手段と、サービス情報暗号用の秘密鍵を生成し、上記秘密鍵を用いて、上記サービス情報を暗号化する手段と、上記全識別子情報列からなる各グループ毎の配付先情報列を導出するための、配付先情報列の導出コードを記憶するためのテーブルと、上記グループ毎の配付先情報列に対応した共通鍵を作成するための共通鍵生成部と、上記グループ毎の共通鍵を用いて、上記秘密鍵を暗号化し、暗号化されたサービス情報に、上記配付先情報列導出コードと暗号化された秘密鍵を同報通信により送出するための手段を有し、

上記各受信局は、情報サービスシステムにおける各受信局が属する各グループの全加入者の識別子を所定の順序で配列した識別子情報列を記憶する手段と、上記情報サービス局が送出した暗号化されたサービス情報と、上記配付先情報列導出コードと暗号化された秘密鍵を受信するための受信部と、上記配付先情報列導出コードから導出される各グループ毎の配付先情報列から、各グループの共通鍵を生成する共通鍵生成部と、上記共通鍵を用いて、上記秘密鍵を復号するための復号部と、各グループの各受信局利用者の各加入者識別子を記憶するための記憶手段とを備え、

該加入者識別子が該グループの上記配付先情報列に含まれていないときに、上記該グループの共通鍵を生成することを禁止することを特徴とする情報サービスシステム。

5．前記受信側共通鍵生成部は、前記受信局に着脱可能な回路装置により構成されることを特徴とする請求項第4項記載の情報サービスシステム。

6．複数の受信局を1つのグループとする複数のグループと、上記複数のグループの複数の受信局に、サービス情報を同報通信によって配布する情報サービス局とからなる情報サービス網のための情報サービスシステムにおいて、

上記情報サービス局は、全加入者の識別子から構成された全加入者の配付先情報列を記憶する手段と、サービス情報暗号用の秘密鍵を生成し、上記秘密鍵を用いて、上記サービス情報を暗号化する手段と、上記各グループ毎の配付先情報列から生成した各グループ毎共通鍵を用いて、上記秘密鍵を暗号化し、暗号化されたサービス情報を同報通信により送出する手段を有し、

上記受信局は着脱可能な回路装置に各加入者の識別子を記憶して、各加入者に配付する手段と、情報サービスシステムにおいて各受信局が属する各グループの加入者の各加入者識別子から構成された配付先情報列を記憶する手段と、上記サービス情報を、上記各受信局に装着された回路装置から出力される各グループの共通鍵を用いて、受信した暗号化秘密鍵を復号化し、上記秘密鍵を用いてサービス情報を復号化する手段を有し、

該回路装置は内部に記憶された該加入者識別子が該グループの上記配付先情報列に含まれていないときに、上記該グループの共通鍵を生成することを禁止することを特徴とする情報サービスシステム。

7．複数の受信局を1つのグループとする複数のグループと、上記複数のグループの複数の受信局に、サービス情報を同報通信によって配布する情報サービス局とからなる情報サービス網のための情報サービスシステムにおいて、

上記情報サービス局は、全加入者の識別子を所定の順序で配列した全加入者の識別子情報列を記憶する手段と、サービス情報暗号用の秘密鍵を生成し、上記秘密鍵を用いて、上記サービス情報を暗号化する手段と、上記各グループ毎

の全加入者の識別子情報列からなる各グループ毎の配付先情報列に対応する複数の加入者識別子からなる配付先情報列を導出するための、配付先情報列導出コードを記憶し、上記グループ毎の配付先情報列に対応した共通鍵を生成し、上記グループ毎の共通鍵を用いて、上記秘密鍵を暗号化する手段と、暗号化されたサービス情報と、上記配付先情報列導出コードと暗号化された秘密鍵を同報通信により送出する手段を有し、

上記受信局は着脱可能な回路装置に各加入者の識別子を記憶して、各加入者に配付する手段と、情報サービスシステムにおいて各受信局が属する各グループの全加入者の識別子を所定の順序で配列した識別子情報列を記憶する手段と、上記暗号化されたサービス情報を、上記各受信局に装着された回路装置から出力される各グループの共通鍵を用いて、暗号化秘密鍵を復号化し、上記秘密鍵を用いてサービス情報を復号化し、

該回路装置は内部に記憶された該加入者識別子が該グループの上記配付先情報列に含まれていないときに、上記該グループの共通鍵を生成することを禁止することを特徴とする情報サービスシステム。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は、同報暗号通信に用いる暗号鍵の配付方式に関する。

〔従来の技術〕

情報化社会の進展と共に、衛星通信やＬＡＮ（ローカルエリアネットワーク）、ＣＡＴＶ（ケーブルテレビ）網等において同報通信を利用して情報通信サービスを行うことが可能になってきた。

情報通信サービスにおいては、映画情報，一般ニュース情報，市況情報，投資情報，ソフトウェア等数多くの情報に対し、情報を送るべき相手に漏れなく正しく情報を伝えることが重要である。さらに、機密性のある情報や高付加価値の情報に対しては、送るべきでない相手には情報が伝わらないようにすることが重要である。

衛星通信等の同報性を持つ通信においては、物理レベルでの送出信号は基本的に受信者全員に伝わる。同報通信において情報の送信先の制御を行うためには、暗号通信を行うことが有効である。

よく知られているように、暗号通信を行う場合には、送信者は暗号化鍵で平文を暗号化してから送信する。受信者は暗号文を受信してから復号化鍵で暗号文を平文に復号化して、本来の情報を得る。暗号化鍵と復号化鍵はペアの関係になっていて、復号化鍵の持ち主のところだけが暗号文を復号化できる。すなわち、本来の情報が伝わる。復号化鍵を持っていないところでは、暗号文が復号化できない。すなわち、本来の情報が伝わらない。

このような暗号通信の特性を利用して、同報通信において送信先の制御を行うことができる。つまり、送信すべき複数の相手のところだけに復号化鍵を持たせるようにしてから、暗号文を同報で送信する。そうすると、送信すべき相手のところにだけ本来の情報が伝えられる。送信すべきではない相手のところには、物理的な信号は伝わるが復号化鍵がないので、本来の情報を得ることはできない。このような暗号通信を利用した限定同報において、次の問題が生じる。つまり、通常同報通信の受信者の数は多く、何千何万と存在する。また、情報サービスすべき情報の種類も多数存在する。

ここで、通信，情報の種類、およびそれをサービスする時刻が異なると、それを受信したいと要求する受信者も異なる。このため、情報サービスをする側にとっては膨大な受信パターンが生じる。受信パターンが異なる毎に、受信者のところの復号化鍵を設定し直すのは情報サービスをする側にとっては大変な負担になる。

ここの問題に対処する従来の技術として、特開昭63－280530号公報に１：Ｎの一方向通信における秘密鍵共有装置が開示されている。

第７図に上記従来例の構成を示す。

この従来例においては、１：Ｎ（Ｎ≧２）の通信を行う場合、次の動作を行う。つまり、３人以

上の双方向の秘密通信を行う際、通信当事者は、それぞれ独立に、自分が保持している秘密鍵共有装置ＣＲの入力端子２７０１から自分以外のグループのメンバーの全ての識別コードＩＤを入力する。例えば、グループのメンバーが、ユーザＡ，ユーザＢ，ユーザＣであるとする。ユーザＡは、自分が保持している秘密鍵共有装置ＣＲの入力端子２７０１から自分以外のグループのメンバー，ユーザＢの識別コードＩＤＢ，ユーザＣの識別コードＩＤＣを入力する。入力端子２７０１から入力された前記識別コードＩＤＢとＩＤＣは、全ユーザに共通な一方向性関数Ｆ（•）発生機2702で一方向性関数Ｆ（ＩＤＢ）、およびＦ（ＩＤＣ）となり、関数比較機２７０４に入力されず、第３のメモリ２７０８に予め入力されているネットワーク、又はデータ通信システムのユーザに共通に与えられている乱数Ｒと、一方向性関数Ｆ(IDA)とを、法２の加算機２７０９で加算し、一方向性関数値ｒ。を得る。

$r_0 = R \oplus F(IDA) \oplus F(IDB) \oplus F(IDC)$

一方向性関数加算値ｒ。は、全ユーザに共通な一方向性関数ｆ（•）発生機２７０６に入力され、

$K_{ABC} = f(r_0)$

となり、秘密通信のための秘密鍵K_{ABC}として、出力端子２７０７から出力される。ユーザＡは、このグループにのみ共通な秘密鍵K_{ABC}を用いて秘密通信を行う。

同様に、ユーザＢは、自分が保持している秘密鍵共有装置ＣＲの入力端子２７０１から自分以外のグループのメンバー，ユーザＡの識別コードＩＤＡ，ユーザＣの識別コードＩＤＣを入力する。入力端子２７０１から入力された前記識別コードＩＤＡとＩＤＣは、全ユーザに共通な一方向性関数Ｆ(•)発生機２７０２で一方向性関数Ｆ(IDA)、および、Ｆ（ＩＤＣ）となり、関数比較機2704に入力されず、第３のメモリ２７０８に予め入力されているネットワーク、又はデータ通信システムのユーザに共通に与えられている乱数Ｒと、一方向性関数Ｆ（ＩＤＢ）とを、法２の加算機２７０９で加算し、一方向性関数値ｒ。を得る。

$r_0 = R \oplus F(IDB) \oplus F(IDA) \oplus F(IDC)$

一方向性関数加算値ｒ。は、全ユーザに共通な一方向性関数ｆ（•）発生機２７０６に入力され、

$K_{ABC} = f(r_0)$

となり、秘密通信のための秘密鍵K_{ABC}として、出力端子２７０７から出力される。ユーザＢは、このグループにのみ共通の秘密鍵K_{ABC}を用いて秘密通信を行う。

ユーザＣは、自分が保持している秘密鍵共有装置ＣＲの入力端子２７０１から自分以外のグループのメンバー，ユーザＡの識別コードＩＤＡ，ユーザＢの識別コードＩＤＢを入力する。入力端子２７０１から入力された前記識別コードＩＤＡとＩＤＢは、全ユーザに共通な一方向性関数Ｆ(•)発生機２７０２で一方向性関数Ｆ（ＩＤＡ），および、Ｆ（ＩＤＢ）となり、関数比較機２７０４に入力されず、第３のメモリ２７０８に予め入力されているネットワーク、又はデータ通信システムのユーザに共通に与えらている乱数Ｒと、一方向性関数Ｆ（ＩＤＣ）とを、法２の加算機2709で加算し、一方向性関数値ｒ。を得る。

$r_0 = R \oplus F(IDA) \oplus F(IDB) \oplus F(IDC)$

一方向性関数加算値ｒ。は、全ユーザに共通な一方向性関数ｆ（•）発生機２７０６に入力され、

$K_{ABC} = f(r_0)$

となり、秘密通信のための秘密鍵K_{ABC}として、出力端子２７０７から出力される。ユーザＣは、このグループにのみ共通の秘密鍵K_{ABC}を用いて秘密通信を行う。

ところで、従来の技術には次の２つの問題がある。例えば、ユーザＡの処理において、秘密鍵共有装置ＣＲにＩＤＢおよびＩＤＣを入力する代りに、ＩＤＢ，ＩＤＣ，ＩＤＡ，およびＩＤＤを入力したとする。ここでＩＤＤは第４のユーザＤのＩＤであるとする。これは、もしユーザＡがそういう意図をもっていれば可能である。この場合加算機２７０９の計算結果は

$r'_0 = R \oplus F(IDA) \oplus F(IDB) \oplus F(IDC) \oplus F(IDA) \oplus F(IDD)$

$$=R\oplus F(IDA)\oplus F(IDA)F(IDB)\oplus F(IDC)\oplus F(IDD)$$
$$=R\oplus F(IDB)\oplus F(IDC)\oplus F(IDD)$$

となる。なんとなれば⊕（排他的論理和）の演算は演算の順序を代えても同じ結果であり、

$$F(IDA)+F(IDA)=0$$

となるためである。このr'_{ABCD}はユーザB，ユーザCとユーザDの間での秘密通信のための秘密鍵である。つまり、ユーザAはそういう意図をもっていれば、自分を含まない他のユーザ間の秘密鍵を得ることができる。このことはネットワークの全ユーザについていえるので、公知例では1：N（N≧2）の通信が行われているときに、本来グループ通信に加わるべきではないユーザでもその気になれば、暗号通信を傍受し復号化できるという問題が生じた。

また、上記従来技術においては、1：Nの暗号通信において、該当するN＋1人のユーザが、具体的にどの相手と通信するかを知るための手段が示されていない。例えば、前述のユーザAの処理において、ユーザAはユーザE，ユーザFとではなくユーザB，ユーザCとグループ通信をするということを知らなければ前記秘密鍵の生成を行うことはできない。公知例では入力端子2701にID情報が入力されることから、だけか一人のユーザが前処理としてユーザ名を関係者に知らせるような処理が想定されるが、1：NのNが大きい場合（例えばN＝1万）、N×IDの長さ分の通信を予め行う必要が生じ、負荷が大である、という問題が生じる。

上述の如き問題点を解決するために、複数のユーザ間で、秘密通信を行うシステムにおいて、第三者がその暗号文を傍受し内容を盗むことができないようにすることを第一の目的とし、さらに、本発明は、複数ユーザが秘密通信を行う度に、相互に各IDを知り合う状態にするため、該ユーザ全員分のIDを含む情報を毎回送らずに済むようにしてシステム全体としての負荷を軽減することを第二の目的とする限定同報用暗号鍵配付方式（特願平1－282960 号）が提案されている。

〔発明が解決しようとする課題〕

ところで、上記限定同報用暗号鍵配付方式は、Nの端末に共通の秘密鍵生成用のデータを、センタがN個の端末に配付し、この秘密鍵生成用のデータから、各端末が公開されているID情報を用いて、秘密鍵を生成する。ここで、公開されているID情報とは、システム参加者の全員のID情報である。従って、システム参加者の数が無制限に大きくなれば、各受信者が秘密鍵を得るために必要な秘密鍵生成用のID情報が無制限に増大し、秘密鍵生成時間も無制限に増大し、システム全体として負荷が大きくなる。

本発明は上記の問題点を解決することを目的としてなされたものである。

〔課題を解決するための手段〕

この問題を解決するために、本発明においては、次の手段をとる。

1．受信者端末を、m個のグループG(i)に分割し、各グループの任意のn個のID情報を入力データとし、各グループに属する受信者のID情報全てに対しハッシュトータルをとり、これを各グループの共通鍵とする。

2．各グループの共通鍵で秘密鍵を暗号化し、暗号化秘密鍵を配付する。

〔作用〕

上記の手段により、次のような効果が得られる。

1．複数のユーザに対し、1：Nの秘密通信を行うシステムにおいて、参加者数が無制限に大きくなっても、各受信者が秘密鍵を得るためには、グループ共通鍵生成用のグループ参加者分のID情報のみを必要とし、ほぼグループ共通鍵生成時間を必要とするだけで、無制限に増大することはなく、システム全体として負荷が大きくなりすぎない。

2．Nの数が増大した場合にも、容易に対処することができ、システムが稼働途中であっても、論理的なグループ数の増加と、情報サービスセンタの若干の負荷増加によって容易に対処できる。

〔実施例〕

第１図～第６図において、本発明の実施例を示す。

〔実施例１〕

第１図は、本実施例のシステム構成を示す図である。

第１図は大きく分けて、情報サービス局１０１，情報利用グループ１０３，情報利用グループ104から構成される。

情報サービス局１０１において、情報サービス装置１０５は、ファイル１０６に蓄積されたサービス情報を、地球局１０７から、衛星通信１０２を介して、論理的にｍ個に分割され、グループの１つである、情報利用グループ１０３の利用者端末１０８，１０９，１１０に、地球局１１１，１１２，１１３を介して、あるいは情報利用グループ１０４の利用者端末１１４，１１５，１１６に、地球局１１７，１１８，１１９を介して配付する。

第１図に示すシステムでは、限定同報通信を、ＩＤベース鍵管理に基づく暗号通信制御によって実現する。つまり、データ送信者である情報サービス局は、受信者のうちＮ人を任意に選んで１：Ｎ通信を行うとき、ＩＤベース鍵管理に基づく暗号通信制御を行う。ＩＤベース鍵管理とは、送信者の識別名、および受信者の識別名をもとに、送受信者だけで共通の暗号鍵を生成する方式である。ここで用いるＩＤベース鍵管理方式は、特願平1－282960で知られている。

第６図（ａ）は、第１図のシステム構成図における情報利用グループ１０３の受信端末者１０８，１０９，１１０の夫々が保持しているか、あるいはグループ１０３として共通に参照可能な公開データの一例を示す。

第６図（ｂ）は、第１図のシステム構成図における、情報利用グループ１０４の受信端末１１４，１１５，１１６の夫々保持しているか、あるいはグループ１０４として共通に参照可能な公開データの一例を示す。

第２図は、第１図のシステム構成図における、情報サービス局の情報サービス装置１０５処理手順を示す。

step201 ：始め

step202 ：秘密鍵Ｋを生成する。

step203 ：ファイル１０６に蓄積されたサービス情報（Ｍ）を、秘密鍵Ｋで暗号化し、これを暗号化データ（Ｃ）とする。

step204 ：秘密鍵Ｋ配付データを生成する。

step205 ：暗号化データ（Ｃ）と秘密鍵Ｋ配付データを、地球局１０７から衛星通信１０２を介して同報通信により配付する。

step206 ：終わり。

第３図は、第２図の処理図における、情報サービス局の秘密鍵Ｋ配付データを生成処理(step204の詳細）手順を示す。

step301 ：始め

step302 ：多数の受信者をｍ個のグループＧ（ｉ）（１≦ｉ≦ｍ）に分割する。

step303 ：ｉ＝０とする。

step304 ：ｉ＜ｍならばstep305 に、ｉ＝ｍならばstep308 に進む。

step305 ：グループＧ（ｉ）のうちの、データ受信者である、ｎ個の端末の共通鍵ＧＫ（ｉ）を、ＩＤベース鍵管理方式によって、送信者の識別名、および受信者の識別名、乱数等をもとに生成する。

step306 ：グループＧ（ｉ）の共通鍵ＧＫ(ｉ)で秘密鍵Ｋを暗号化し、これをＫ’（ｉ)とする。

step307 ：ｉ＝ｉ＋１

step308 ：グループＧ（ｉ）（１≦ｉ≦ｍ）の共通鍵ＧＫ（ｉ）生成用のデータと、暗号化秘密鍵Ｋ’（ｉ)を編集し、これを秘密鍵Ｋ配付データとする。

step309 ：終わり。

第４図は、第１図のシステム構成図における、情報利用端末の処理手順を示す。ここでは、端末１０８の処理を示す。

step401 ：始め

step402 ：情報サービス局より配付された限定同報データを受信する。

step403 ：秘密鍵Ｋ配付データのうち、受信者

１０８が属するグループ１０３の制御情報を読みとり、端末１０８の属するグループG（ｉ）の鍵配付データに対応するＩＤ情報を、第６図（ａ）のグループ共通の参照可能な公開データを読みだす。

step404 ：ＩＣカードをコールし、共通鍵ＧＫ（ｉ）を生成する。

step405 ：共通鍵ＧＫ（ｉ）で、暗号化秘密鍵K′（ｉ)を復号化し、秘密鍵Ｋを得る。

step406 ：秘密鍵Ｋで、暗号化データ（Ｃ）を復号化し、データ（Ｍ）を得る。

step407 ：終わり。

第５図は、第２図の処理図における、情報サービス局の秘密鍵Ｋ配付データの構成例を示す。

秘密鍵配付データは、グループ１の識別子と、グループ１の配付先制御情報と、秘密鍵Ｋを配付先制御情報に対応したＩＤ情報で生成したグループ１の共通鍵で暗号化した暗号化秘密鍵K′（1)、およびグループ２～グループｍについて、同様に生成されたデータから成る。

本実施例実行の結果、各グループの受信者は、情報サービスシステムの全ての参加者の依存するのではなく、各グループの情報サービスシステム参加者にのみ依存して、共通鍵を生成することができる。従って、情報サービスシステムへの参加者の増減に、容易に対処することができる。

〔変形例１〕

実施例１の第５図の密秘鍵Ｋ配付データにおいて、各グループの識別子を使用せず、所定の配列を用いることにより、各グループの配付先制御情報を読み込む。

本変形例実行の結果、情報サービス局が生成，管理する秘密鍵Ｋ配付データを短くすることができる。

〔変形例２〕

実施例１の第５図の密秘鍵Ｋ配付データにおいて、各グループの識別子，暗号化された秘密鍵の他に、各グループの共通鍵生成で用いた乱数等のデータを含ませる。

本変形例実行の結果、グループ共通鍵の種類を、秘密鍵を配布する時刻や、配付する秘密鍵の種類に応じて、生成するグループ共通鍵を変えることができる。

〔実施例２〕

グループ１０３の受信端末者１０８が、鍵生成用のＩＣカードと、グループ１０３の参加者のＩＤ情報を持って、移動先のグループ１０４の受信端末１１７から、情報サービスを受ける場合にも、実施例１と同じ効果もたらすことが可能である。

本実施例実行の結果、移動先での情報サービスの利用を容易に実現できる。

〔変形例３〕

グループ１０３の受信端末者１０８が、鍵生成用のＩＣカードのみを保持していて、グループ１０３の参加者のＩＤ情報を持っていない状況下で、移動先のグループ１０４の受信端末１１７から、情報サービスを受ける場合に、グループ103の正規の受信端末者１０９、あるいは正規の鍵共有サービスを行う受信端末者１１０が得た秘密鍵を、受信端末者１０９と移動先の受信端末者108との間で、ＩＤベース鍵管理に基づく暗号通信制御によって共有することも可能である。

本変形例実行の結果、グループのＩＤ情報を充分に持たない場合にも、正規の受信端末者のサービスによって、秘密鍵を容易に得ることができる。

〔変形例４〕

変形例１において、鍵生成用のＩＣカードが通信機能をもち、移動先から情報サービスを受ける場合に、同グループの正規の受信者が得た秘密鍵を、正規の受信者のＩＤ情報からＩＤベース鍵管理に基づく暗号通信制御によって共有することも可能である。

本変形例実行の結果、グループのＩＤ情報を充分に持たない場合にも、正規の受信端末者のサービスによって、秘密鍵を容易に得ることができる。

〔発明の効果〕

本発明により、次のような効果が得られる。

１．複数のユーザに対し、１：Ｎの秘密通信を行うシステムにおいて、第３者がその暗号文を傍

受し、内容を盗むことを防止できる。

2．システムが稼働途中に、Ｎの数が増大した場合にも、論理的なグループ数の増加と、情報サービス局の若干の負荷増加によって容易に対処することができる。新たな情報利用者の参加に伴って、各情報利用者の保持するＩＤ情報をアップデートする必要がない。

3．実システムを想定して、高速化，負荷の縮小が求められる受信端末側の鍵生成時間を試算したところ、次の結果を得ている('９０　ＣＩＳ限定同報暗号通信による、ソフトウェア配布保護の一方法、宝木他、参照）。

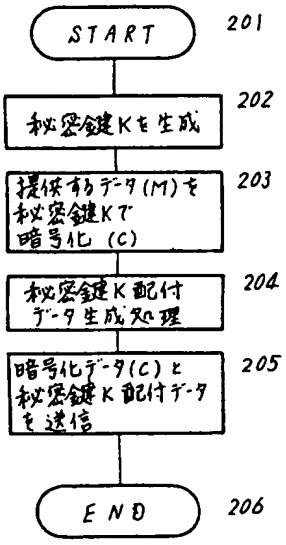
すなわち、１グループの構成を１０００端末とし、１対１０００の暗号通信の場合、ＩＣカード内部で一つの暗号鍵を生成するのに要する時間は、６４ビット×１０００／８０Ｋｂｐｓ＝０.８秒程度となる。ただし、この処理の前に、６４ビット×１０００＝６４Ｋビットのデータを ＩＣカードに入力する必要があり、このため、少なくとも６４Ｋビット／９.６Ｋｂｐｓ＝６.７秒のＩ／Ｏ時間を要する。従って、１対１０００の限定同報暗号通信を行うとき、２個の暗号鍵を共有するためには、６.７＋０.８×２＝８.３秒以上をＩＣカードのところで費やすことになる。しかし、この８.３秒＋α のロス時間は、通常、計算機プログラムのダウンロードが発生する間隔やダウンロードに関する時間に比べて小さく、許容できるものである。

上記の例を用いて、システムの参加者を10000000端末を想定し、論理的に１００００グループに分割する場合を考える。情報サービス局が生成し、配付する秘密鍵Ｋ配付データは、10000000ビット（配付先情報）＋６４ビット（暗号化秘密鍵データ）×１００００＋８ビット（グループ鍵別子）×１００００＝１０.７２０Ｍビット程度となる。衛星通信を利用した場合、１５Ｍｂｐｓ程度以上は可能であり、秘密鍵Ｋ配付データの受信は１秒程度と考えられる。各グループの共有鍵生成時間は、上記の結果から約８.３秒、共通鍵による暗号化秘密鍵の復号処理速度は2.7Ｍｂｐｓ（暗号方式として、ハイセキュリティーマルチ：Hisecurity-Multiを使用）である。従って、情報サービス局のサービス開始から、各端末が秘密鍵を得るまでの時間は１０秒程度で可能となり、本システムでの共有鍵生成時間は、システムの参加者の数にほとんど影響されない。システムの参加者の増加にほとんど無関係に、情報利用者の鍵生成時間が保証される。

4．図面の簡単な説明

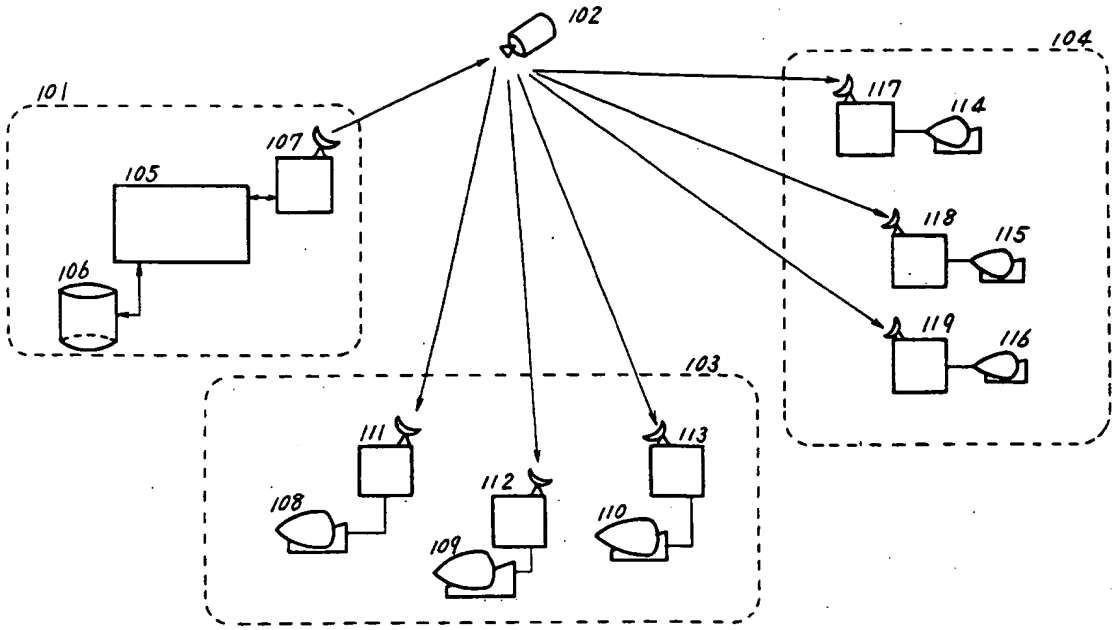
第１図は、本発明の実施例のシステム構成を示す模式図、第２図，第３図は、第１図のシステム構成において、情報サービス局の処理の概要を示すフロー図、第４図は、情報利用者の処理の概要を示すフロー図、第５図は、第２図の配付データのうち、送信先制御情報と暗号化秘密鍵データを示す図、第６図は、グループＧ（ｉ）の各端末が保持するＩＤ情報の一例を示す図、第７図は、従来方法を示すブロック図である。

第２図

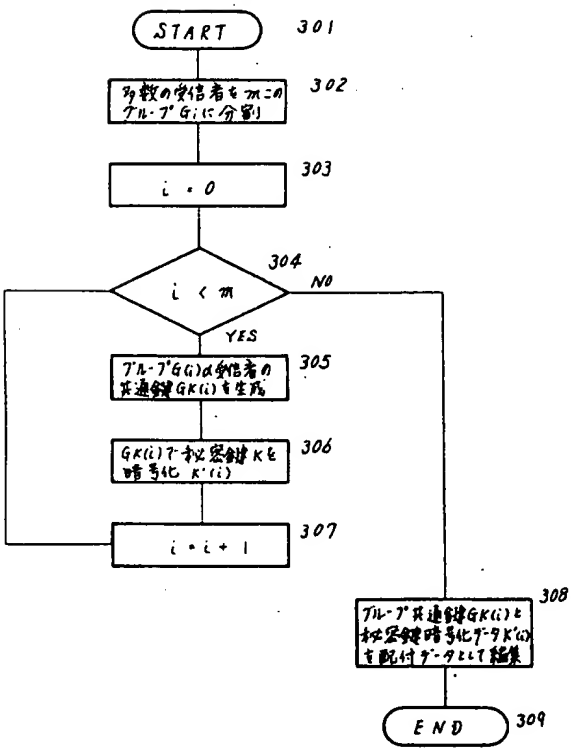


代理人　弁理士　小川勝男

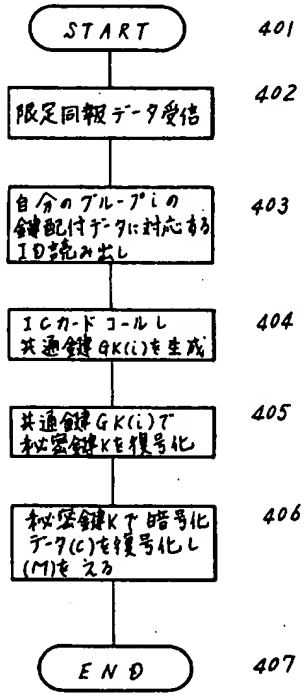
第 1 図


102
104
101
117
114
107
105
118
115
106
119
116
103
111
113
108
112
110
109

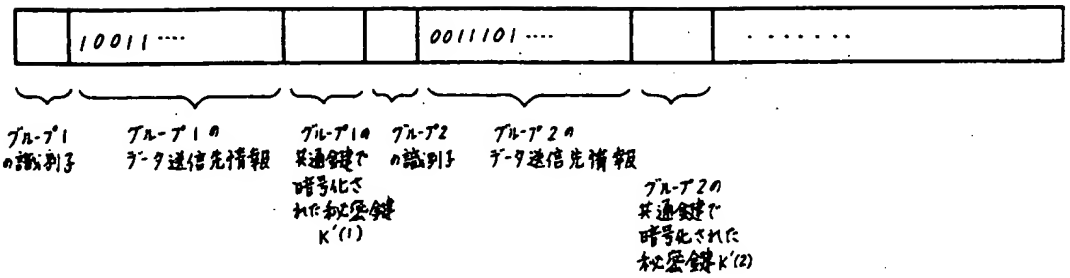
第 3 図


START
301
多数の受信者をm個のグループGiに分割
302
i ← 0
303
i < m
304
NO
YES
グループG(i)の受信者の共通鍵GK(i)を生成
305
GK(i)で秘密鍵Kを暗号化 K'(i)
306
i ← i + 1
307
グループ共通鍵GK(i)と秘密鍵暗号化データK'(i)を配付データとして編集
308
END
309

第 4 図


START
401
限定同報データ受信
402
自分のグループiの鍵配付データに対応するID読み出し
403
ICカードコールし共通鍵GK(i)を生成
404
共通鍵GK(i)で秘密鍵Kを復号化
405
秘密鍵Kで暗号化データ(C)を復号化し(M)をえる
406
END
407

第 5 図



第 6 図

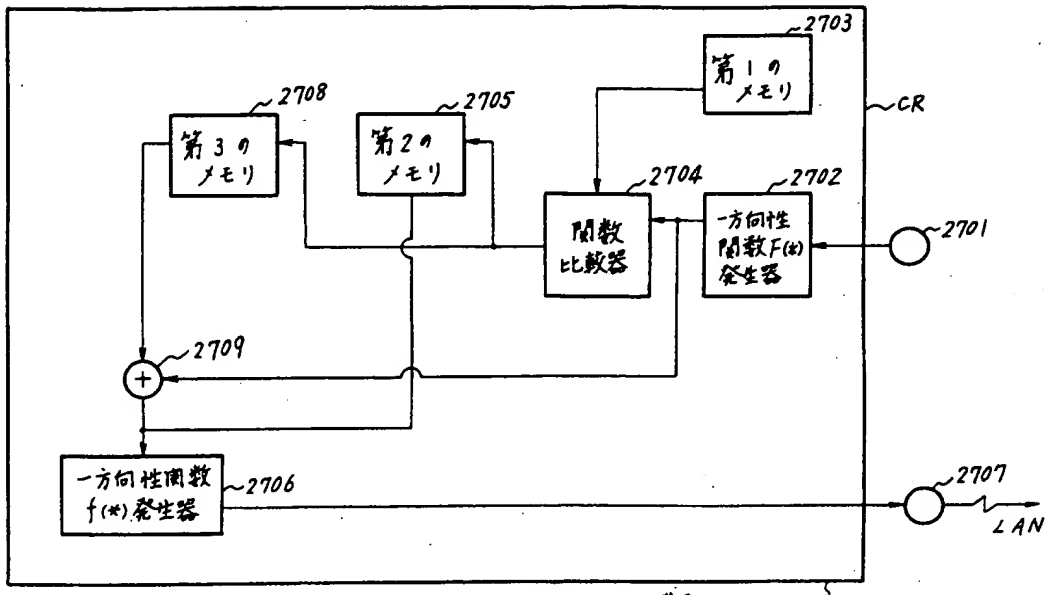
(A)

ユーザ名称	ID 情報
IC1-001	900205YASUK
IC1-002	890907OKADA
IC1-003	H. YA890108*
⋮	⋮

(B)

ユーザ名称	ID 情報
IC2-001	56F013AB42D381FE
IC2-002	J. G * 62080301
IC2-003	システム 1268-123
⋮	⋮

第 7 図



2701　入力端子
2707　出力端子
2709　法2の加算器